

SECRET INFORMATION STORAGE DEVICE

Patent number: JP2000029792
Publication date: 2000-01-28
Inventor: TOMIZAWA SATOSHI
Applicant: HITACHI LTD
Classification:
 - international: **G06F12/14; G06F12/14; (IPC1-7): G06F12/14**
 - european:
Application number: JP19980195353 19980710
Priority number(s): JP19980195353 19980710

Report a data error here

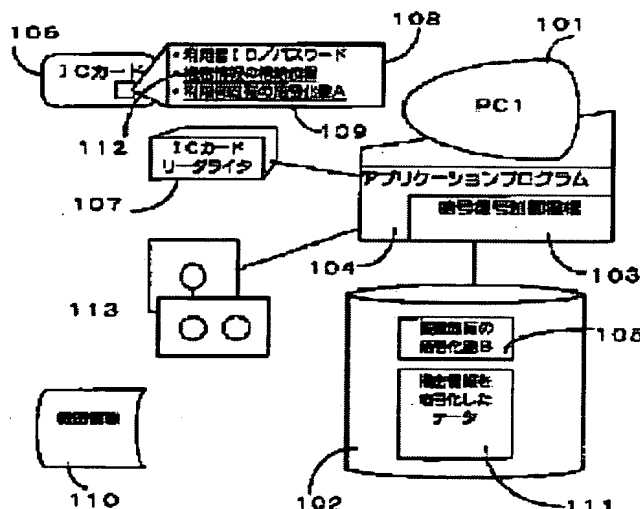
Abstract of JP2000029792

PROBLEM TO BE SOLVED: To improve the confidentiality by storing information on a user, information showing the storage destination of secret information, and an encoding key characteristic of the user on a small-capacity medium and generating and storing a key characteristic of the user on a hard disk.

SOLUTION: At incorporating, a key B105 characteristic of the device is generated and stored on an external storage device 102.

Then the user actuates an encoding control mechanism 103 to register information 108 on the user. The contents of the information 108 of the user consist of a user ID, a password, and the encoding key A109 characteristic of the user. Then the user specifies desired secret information 110 to be concealed. An encoding control mechanism 103 reads the secret information 110 out and encodes it with a key A109 characteristic of the user.

Consequently, a file obtained by further encoding the obtained file with the encoding key 105 characteristic of the device is written to a location such that the user specifies on the external storage device of the device. The location that the user specifies is written as a storage location 112 of the confidential information to an IC card 106.



Data supplied from the esp@cenet database - Worldwide

特開 2 0 0 0 - 2 9 7 9 2

(P2000-29792A)

(43) 公開日 平成12年1月28日(2000.1.28)

(51) Int. Cl.	識別記号	F I	テーマコード(参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14 3 2 0 C	5B017

審査請求 未請求 請求項の数 3 O L (全 8 頁)

(21) 出願番号 特願平10-195353

(22) 出願日 平成10年7月10日(1998.7.10)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 富澤 智

神奈川県川崎市幸区鹿島田890番地
会社日立製作所情報システム事業部内

株式

(74) 代理人 100068504

井理士 小川 勝男

Fターム(参考) 5B017 AA06 BA05 BA07 CA14

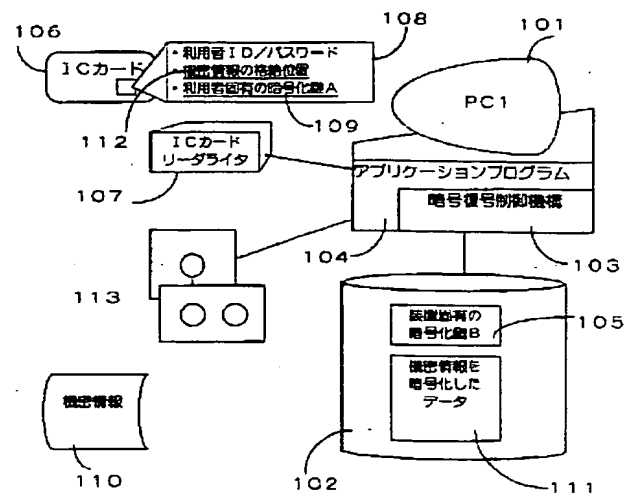
(54)【発明の名称】機密情報格納装置

(57) 【要約】

【課題】格納された利用者の情報と利用者の入力情報を突き合わせて正しい時、機密情報にアクセスするための鍵を取出す方法などでは、利用者の情報と機密情報または機密情報にアクセスする鍵が同一の媒体に格納され悪意の第三者により媒体自体が盗まれた場合、総当たり的な方法で利用者の機密情報または機密情報にアクセスするための鍵を取出すことができる危険性がある。

【解決手段】本発明では機密情報を格納する時に利用者固有の鍵と装置固有の鍵とを使用することにより、暗号化し、より機密性の高い情報の格納方法を提供するものである。

❖ 1



Aを用い利用者情報が正しく入力された時のみ、鍵Bの復号化処理を行った出力ファイルを複写先の媒体に格納する機能を持たせる。複写先の媒体から別の装置のハードディスクに格納するには、媒体Aを用いて利用者登録した後、媒体Aと利用者の正当な入力があった時、初めて装置固有の鍵で暗号化してハードディスクに格納する機能により実現する。

【0010】

【発明の実施の形態】以下本発明実施の具体的方法を示す。

【0011】図1は本発明を適用する装置とその構成を示している。以下では携帯性に優れた比較的小さい媒体をICカード、装置本体に固定的に接続される外部記憶装置をハードディスクとして記述する。本発明において、暗号化制御機構103はコンピュータ装置101の外部記憶装置102にアプリケーションプログラム104に含まれて組み込まれる。例えばアプリケーションプログラムは電子証明書が必要とする電子商取引のクライアントなどが考えられ、機密情報は電子証明書などが想定できる。

【0012】組み込みの際には、装置固有の鍵B105を作成し外部記憶装置102に格納する。装置固有の鍵B105の作り方は組み込まれた日付時刻やハードウェア固有のアドレス情報、あるいは乱数を用いて、他の装置と同一になる可能性が十分に小さいと判断できる方法で行う。

【0013】次に利用者が暗号化制御機構103を起動し利用者の情報を登録する。このとき暗号化制御機構103はICカードリーダーライタ107により、初期化されたICカード106内に利用者の情報108を書き込む。利用者の情報108の内容は利用者ID/パスワード、利用者固有の暗号化鍵A109である。次に利用者が隠蔽しようとする機密情報110を指定する。

【0014】これは多くの場合外部媒体112により読み込まれる。暗号化制御機構103は機密情報110を読み取り利用者固有の鍵A109により暗号化する。この結果、得られたファイルを更に装置固有の暗号鍵105により暗号化した結果得られたファイルを装置の外部記憶装置内の利用者が指定した位置に書き込む。利用者が指定した位置はICカードの中に機密情報の格納位置112として書き込まれる。

【0015】以下、それぞれの処理の詳細を説明する。図2にアプリケーションプログラム104のインストール処理のフローを示す。プログラムのインストールを開始すると通常のインストールと同様にプログラムの組み込み201を行う。201には必要なディレクトリの作成、必要なプログラムファイル等の圧縮解凍および複写、プログラム動作環境変数の設定、レジストリの設定等が含まれる。

【0016】201が終了した後、装置固有の暗号鍵B

の生成202、鍵Bのハードディスクへの格納203を行いインストール処理を終了する。図3は利用者登録処理の流れを示している。まず利用者情報の読み込み（利用者ID）301、利用者情報の読み込み（パスワード）302を行う。これらは利用者による画面入力を読み取る方法で実施する。

【0017】次にICカードを読み取り303、データが既に存在する場合は初期化してよいかどうかを利用者に判断させる（304、307）。その後利用者固有の暗号鍵Aを生成305し、利用者情報、暗号化鍵AをICカードに書き込む。図4は機密情報の格納処理1を示す。機密情報格納処理1は全く機密情報が暗号化されていない状態から暗号化されハードディスクに格納されるまでの処理である。

【0018】まず利用者情報、ICカードの読み込み（401、402）利用者の入力が正しいかを判定し403、正しければ機密情報の読み込み404、ICカードから暗号化鍵Aを取出し405、暗号化鍵Aで機密情報を暗号化406する。

20 【0019】次にハードディスクから装置固有の暗号化鍵Bを取出し、鍵Aで暗号化された機密情報をさらに暗号化鍵Bで暗号化408する。最後に暗号化された機密情報の格納位置を利用者に問合わせ409、指定された格納位置情報をICカードに書き込む410とともに暗号化した機密情報を指定された格納位置に格納411する。なお、利用者情報の入力が正しくなく規定回数を超えた誤入力があった場合は処理を中止する（412、413）。

30 【0020】図5、図6は上記で格納された暗号化された機密情報を別の媒体に複写する処理の手順と同様の機能がインストールされた別の装置のハードディスクに媒体を経由して機密情報を格納する方法を示す。図5の複写処理では、まず利用者情報の読み込み501、ICカードの読み込み502を行い入力が正しかった場合503は、ICカードから格納位置情報を読み取り504、格納位置に格納された暗号化された機密情報を読み込み505、暗号化鍵Bを取出し506、機密情報の暗号化鍵Bによる復号化507を行う。次に複写先の位置を利用者から画面入力させ508、鍵Bで複合された機密情報（鍵Aで暗号化されている）を複写先に指定された媒体に格納509する。利用者情報の入力誤りは図4と同様（510、511）。

40 【0021】図6の機密情報格納処理2（別の装置への格納処理）では、まず利用者情報の読み込み601、ICカードの読み込み602、利用者の入力が正しかった場合603には、入力元ファイルの位置情報を利用者に入力させ604、暗号化鍵Bで復号化された機密情報（暗号化鍵Aで暗号化されている）を入力元ファイルの位置から読み込み605、暗号化鍵B'を取出し606（鍵B'：別の装置であるため鍵Bと異なることを意味す

50

【图 2】

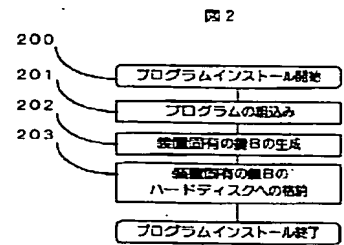
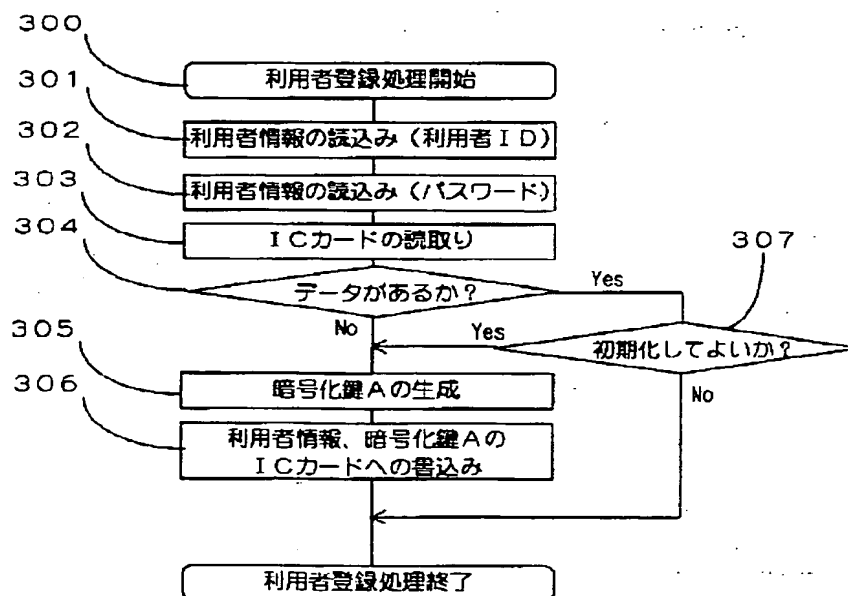


图 3



【図5】

図5

